統合機能の設計上の考慮事項

シングル サインオン（SSO）に関する考慮事項

シングル サインオン機能は、コンタクト センター ソリューションのすべてのアプリケーションとサービスに対して、ユーザを認証して承認します。認証とは、ユーザの身元（「ユーザが主張どおりの本人であること」）を立証するプロセスです。承認とは、認証済みユーザに対してユーザが要求したアクションの実行を認めるプロセスです（つまり、「ユーザは要求したことを実行できます」）。コンタクト センター ソリューションで SSO を有効にすると、ユーザは 1 回サインインするだけで、各自のすべてのシスコ ブラウザベースのアプリケーションとサービスにアクセスできます。SSO により Cisco Administrator アプリケーションにアクセスすることはできません。

コンタクトセンター ソリューションに対して SSO をサポートするには、セキュリティ アサーション マークアップ言語 2.0（SAML v2）Oasis 標準と互換性がある ID プロバイダー（IdP）をインストールして設定する必要があります。現在サポートされている ID プロバイダー製品のリストおよびバージョンについては、『*Compatibility Matrix for Cisco Unified CCX*』（http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCX）を参照してください。

コンタクト センター ソリューションに対する認証と承認は、Cisco Identity Service（Cisco IdS）によって管理されます。SSO を使用できるユーザがサインインすると、Cisco IdS は、最初に ID プロバイダー（IdP）とやり取りしてユーザを認証します。IdP はユーザ プロファイルを保存して認証サービスを提供し、SSO サインオンをサポートします。ユーザが認証されると、Cisco IdS はユーザがアクセスを試みているシスコ サービスと情報を交換し、ユーザがその要求しているロールに対して承認されていることを確認します。ユーザが認証および承認されると、Cisco IdS は、アプリケーションへのユーザのアクセスを許可するアクセス トークンを発行します。特定のセッション中にアクセスが確立されると、ユーザは、クレデンシャルを再提示することなく、コンタクト センター ソリューションのアプリケーションを切り替えることができます。

（注） ユーザ クレデンシャルは IdP にのみ提示されます。コンタクト センター ソリューションのアプリケーションとサービスはトークンのみを交換します。ユーザの情報は確認しません。

IdP をコンタクト センター ソリューションと統合するには、次の管理タスクを実行します。

- Cisco IdS と ID プロバイダー間に信頼関係を確立する。
- システムで SSO モードを設定し、SSO に対してユーザを有効にする。
- [シングル サインオン（Single Sign-On）] Web ページで登録して、シングル サインオン コンポーネントをオンボードする。
- [シングル サインオン（Single Sign-On）] Web ページで [SSO セットアップのテスト（Test SSO Setup）]を実行し、各コンポーネントの登録状態をテストする。認証のために ID プロバイダーにリダイレクトされます。[SSO セットアップのテスト（Test SSO Setup）]が成功すると、[有効（Enable）] オプションが有効になります。

SSO メッセージ フロー

SSO ユーザのアクセス トークンは、対応するアプリケーションにアクセスするユーザを検証するために Cisco IdS によって発行されます。ユーザが有効であると判明すると、各アプリケーションによってローカルに承認が実行されます。Cisco IdS は OAuth 2.0 で定義された承認コード付与フローをサポートしており、承認コードを発行する前に SAML v2.0 を使用してユーザを認証します。

ユーザが SSO 対応サービスの Web ページを参照すると、認証要求が Cisco Identity Service にリダイレクトされます。Cisco Identity Service は、SAML 認証要求を生成して ID プロバイダーに渡します。IdP は、ユーザに対してブラウザにサインイン ページを表示し、ユーザのクレデンシャルを収集します。IdP はユーザを認証すると、Cisco IdS に SAML アサーションを発行します。アサーションには、ユーザに関する信頼できるステートメント（ユーザ名や権限など）が含まれています。

アサーションには属性が必要です。Cisco IdS は uid と user principal を抽出し、承認コードを生成して SSO 対応アプリケーションに提供します。承認コードを受け取ると、アプリケーションはアクセス トークンと更新トークンの ID を要求します。

アクセス トークンはユーザ情報を検証するためにアプリケーションで使用され、更新トークンは新しいアクセス トークンを要求するために使用されます。これらのトークンのそれぞれに有効期間が関連付けられています。

（注） 新しいアクセス トークンと更新トークンのペアは、承認コードが期限切れになる前にのみ取得できます。

アクセス トークンは、現在のアクセス トークンと更新トークンの両方が有効で期限が切れていない場合にのみ更新できます。

更新トークンの期限が切れている場合は、アクセス トークンを更新できません。つまり、再び認証を受け、承認コードを再要求する必要があります。

認証プロバイダーにユーザ クレデンシャルを提示している間にだけ、SAML と OAuth によるユーザの認証が可能になります。ユーザ名とパスワードは IdP にのみ提示されます。コンタクト センター ソリューションのアプリケーションとサービスはユーザ情報を確認しません。SAML アサーションと OAuth トークンのみが交換されます。

シングル サインオンのハイ アベイラビリティに関する考慮事項

コンタクト センター ソリューションのコア コンポーネントごとに、ハイ アベイラビリティ モードをサポートする Cisco Identity Service クライアントがあります。どの SSO 対応アプリケーションも、ローカルまたはリモートの Cisco Identity Service インスタンスに接続できます。

デフォルトでは、Cisco Identity Service のローカル インスタンスに接続します。ローカル Cisco Identity Service は、ローカルに実行されるデフォルトの優先 Cisco Identity Service です。

リモート Cisco Identity Service が設定されている場合、Cisco Identity Service クライアントは、ローカル Cisco Identity Service で障害が発生したときにフェールオーバーをサポートします。ローカル Cisco Identity Service が再び使用可能になると、Cisco Identity Service クライアントはローカル Cisco Identity Service にフェールバックします。

次の表は、ローカルおよびリモート Cisco Identity Service のさまざまな状態における、Cisco Identity Service クライアントのフェールオーバーとフェールバックの詳細を示しています。

表 *1*：*Cisco Identity Service* の状態に基づく *Cisco Identity Service* クライアントのフェールオーバーおよびフェールバック シナリオ

ローカル Cisco Identity Service	リモート Cisco Identity Service	Cisco Identity Service クライアントの接続先
IN_SERVICE	N/A	ローカル Cisco Identity Service
PARTIAL_SERVICE	IN_SERVICE	リモート Cisco Identity Service
PARTIAL_SERVICE	PARTIAL_SERVICE	ローカル Cisco Identity Service
OUT_OF_SERVICE	PARTIAL_SERVICE	リモート Cisco Identity Service
OUT_OF_SERVICE	OUT_OF_SERVICE	なし

OUT_OF_SERVICE	未設定	なし

シングル サインオンの設計への影響

この項では、シングル サインオン（SSO）機能が設計に及ぼすいくつかの影響について詳しく説明します。実装では、すべての Web アプリケーションへのアクセスに HTTPS プロトコルだけを使用する必要があります。SSO が有効になっている場合、Web アプリケーションへの HTTP アクセスはサポートされません。

Unified CCX での認証モード

SSO の実装について決定する際には、次の 2 つの認証モードから選択できます。

- **SSO**：SSO の展開で**すべての**エージェント、スーパーバイザ、管理者（Cisco Unified CCX Administration または Cisco Unified CCX Serviceability アプリケーションの管理者）が有効になります。
- **非 SSO**：既存の Unified CM ベースのアプリケーションまたはローカル アプリケーションを使用します。

SSO モードのアプリケーション

- Cisco Unified Intelligence Center（CUIC）
- Cisco Finesse
- Cisco Finesse でホストされるガジェット
- Cisco Unified CCX Administration
- Cisco Unified CCX Serviceability

（注） Cisco Finesse IP Phone Agent は、SSO 対応モードではサポートされません。

SSO 非対応のアプリケーション

次のアプリケーションはシングル サインオンに対応していません。

- Cisco Finesse Administration
- Cisco Identity Service Administration
- Disaster Recovery System
- Cisco Unified OS Administration
- Cisco Unified Serviceability

- スタンドアロン Cisco Unified Intelligence Center
- Cisco Unified CCX Editor
- Real Time Monitoring Tool
- Cisco SocialMiner
- Cisco Media Sense
- Cisco Workforce Optimization
- サードパーティのすべてのアプリケーション